An Exploratory Study on Causes of Identity Document Theft in South Africa

William Moyahabo Rakololo[1] and Witness Maluleke[2,*]

[1]Forensic Investigator at Department of Rural Development and Land Reform, South Africa

[2]Department of Criminology and Criminal Justice, University of Limpopo, South Africa

Abstract: This study explores the causes of Identity Document (ID) theft in South Africa, the focus is concentrated to Polokwane Central Business District (CBD), Bendor Park, and Flora Park, and the number of stores situated in the business sectors of these areas. From a quantitative standpoint, 90 respondents were selected in this study. The findings indicate that conceptual understanding of this crime (ID theft) can play a pivotal role in addressing the manifestation of this crime in a large extent as nature and extent can be established, the use of technological means also contribute to ID theft, this is also linked to individuals (victims) ignorance. For recommendations; the use of technology and conventional method in awareness can help in responding to the scale and consequence of ID theft in the Polokwane Policing Area effectively.

Keywords: Awareness, Causes [of identity theft], Identity Document theft, Polokwane area, South Africa.

INTRODUCTION

Identity theft is something the latest; law enforcement agencies have been struggling with this scourge for a long time. However, it is acknowledged that the induction of the internet into mainstream society and commerce, this crime took new dimensions. This crime can take different forms, notably in a form of stealing people's data relating to Social Security (SS) numbers, login names and passwords, driver's license numbers, and bank account information. The stolen information can be often used for fraud unlimited to tax returns, medical fraud, and digital impersonations (Forensics Colleges, 2020). The ID theft occurs when the personal details of individuals are deliberately used without consent, this involves the name and [personal] information of an individual or juristic person used to gain financial benefits or cause financial loss to the impacted party. It is also affirmed that this type of fraud may cause financial and reputational losses to impacted parties, which may continue to be unchecked for a long duration of time, Southern African Fraud Prevention Service [SAFPS] (2020). Law for All (2020) collaborated that ID theft in South Africa takes place when potential criminals steal personal information for their benefit. The-said criminals fraudulently use victims' ID to obtain credit, loans, or other benefits in the victim's name, [often] resulting in a mountain of debt. Some criminals often steal another's identity to hide their own, with the 'new' ID used to obtain employment as a foreign citizen, claim social grants, escape criminal prosecution and to claim life insurance policy benefits. Furthermore, the Forensics Colleges (2020) highlights that the common consequences of this crime relate to compromised debit and credit card information. The continued increase of ID theft worldwide potentially holds detrimentally consequences for possible victims of this crime, the economic impact can decrease consumers' confidence globally. Thus, awareness training is regarded as a possible single most important activity to reduce ID theft as there is no single perfect solution to safeguard potential victims from a possible risk of ID theft and all indications suggest that ID theft is going to escalate rather than disappear (Forensics Colleges, 2020). The reported transformations related to the accumulations, recording, storing, and dissemination of using network media of information and knowledge changed the standards of living. The technological advancements, with Information Technology (IT) adoption, changed the world while bringing it to new possibilities of security risks for fraudsters to commit ID theft based on stealing and using another person's ID for fraudulent purposes. Correspondingly; a single corporate database may yield hackers millions of records, which may have catastrophic consequences for victims and credibility of a compromised business and personal wellbeing (Augustyn, 2005).

Cassim (2015) provides that the inception of the internet provided instant and cheap communication across the world, further, making it easier for individuals to transact across a multitude of jurisdictions. The resultant risks and dangers of the internet subjected individuals to become vulnerable to cyber-attacks and ID theft. Sophisticated organised

*Address correspondence to this author at the Department of Criminology and Criminal Justice, University of Limpopo, South Africa; Tel: 015 268 4881; E-mail: witness.maluleke@ul.ac.za

E-ISSN: 1929-4409/20

criminal networks use cyberspace to commit new criminal behaviours targeting against susceptible and vulnerable computer users who use the internet to conduct their daily activities, such as sending electronic-mails (e-mails), purchasing goods, and chatting on social networking sites, as well as those who opt for the traditional methods of living their lifestyles. Furthermore, the speed of the internet also brought challenges to lawmakers in terms of regulating and responding to this crime effectively. The anonymity of the internet also facilitated cybercrimes such as ID theft. This often occurs when a person's personal information, such as an ID is wrongfully obtained and thereafter used to commit theft or fraud. Identity theft can be committed without technical means via physical or traditional means or by mail theft or online. The ID thief uses the information, among other things to open credit accounts, open bank accounts, purchase merchandise, and rack up debts amounting to millions of rand in the victims' names. Thus, personal information is criminally obtained by ID theft and the ID thieves also use the ID-related information or data to commit unlawful activities in the victims' names. The ID thieves involved operate in a multi-jurisdictional environment, which makes the tracking and prosecution of such offenders difficult and problematic.

Traditionally, the ID theft happens when someone illegally obtains another person’s hardcopy of a government-issued ID (www.doc.gov.za). From this definition, it can be concluded that ID theft is the acquisition of an individual’s personal and identifiable information to commit fraud or theft without the person’s knowledge. Taking into consideration the consulted literature and theories, various researchers (Angeloupou, 2010:2; Newman and McNally, 2005:1; Ruppar, 2005:5; Allison, Schuck and Lersch, 2004:19; and Allison, 2003:3) reached a consensus that ID theft refers to the unlawful use of another person's ID unique to such individual to commit a fraudulent act. In conjunction with this definition, Allison, *et al.* (2005:19), further emphasise that “unlawful” in this context constitutes the unauthorised use of another’s personal information with criminal intent. According to Ruppar (2005:5), a victim's ID can be used for both financial gains and to physically misrepresent the victim to people such as law enforcement officials, employers, or medical providers.

For this study to be precise and fall within the ambit of the definition of ID theft in the paragraph above, the present researchers limited the definition of ID theft to the following areas:

- The unlawful use of another person’s ID book or card;
- The unlawful use of another person’s birth or death certificate;
- The unlawful use of another person’s passport; and
- The unlawful use of another person’s driver’s licence.

The limitation allowed the researchers to be specific and interpret the results accurately. Moreover, the unlawful use of the above-referred documents is prejudicial to the next individual thus constituting ID fraud. Hence, the interplay between ID theft and ID fraud is highlighted in this study.

Ruppar (2005:5) states that ID theft has become such a widespread threat to human security that the subject matter pervades current popular culture. Yet, even though ID theft has become a part of society’s vocabulary, information on how to prevent and protect individuals from ID theft is pervasive (Ruppar, 2005:5). As such, the researchers are of the view that this new trend of crime has massively grown to its exponential level as observed and experienced, particularly in South Africa and generally throughout the globe (Joseph, 2013:1). The latter statement is supported by the probabilities that ID theft could be costing South Africa more than R1-billion every year, according to a major credit bureau and a national insurance organisation (Joseph, 2013:1).

PRELIMINARY LITERATURE REVIEW IDENTITY DOCUMENT THEFT

The Nature and Extent of Identity Document theft

Miri-Lavassani, Kumar, Movahedi, and Kumar (2009:364) believe that many things have changed since the early nineteenth century, yet many things have remained the same. The non-monetary contents of a purse or wallet, such as ID cards, can be used by ID thieves to damage the good name, i.e. credit record of ID fraud victims and make them poor indeed. Thus, some authors (Koops, Leenes, Meints, Van der Meulen and Jaquet-Chiffelle, 2009:1; Murphy, 2003:4; Hinde 2005:188; Holt and Turner, 2012:308; Joseph, 2013; and Roberds and Schreft, 2009:918) agree that the theft of IDs has exponentially increased in recent years and is the fastest-growing white-collar crime in many countries, especially in developed countries.

Approximately one billion parts of personal information were lost in South Africa in 2014, costing the country R432 256 000. Unfortunately, cyber thieves increased their deeds in 2015, with costs escalated to R465 412 000 in July. The societal challenge lies in minimising chances of becoming part of these statistics (Michau, 2017). The SAFPS (2019) statistics indicated a sharp increase in ID theft. The fraudsters reported being using fabricated identification ID's and names decreased by 48% when compared with 2018. However, the impersonation of using real ID's and names increased by 99% on 2018 figures. The combined use of forged documents by fraudsters, including falsified employment details, forged payslips, and false qualifications increased drastically. The 2018 figures highlighted an increase of 47% on 2017 figures, while there was an increase of 33% in 2019 on 2018's reflected figures (Staff Writer, 2019).

According to Anderson (2006) (in Copes, Kerley, Huff and Kane, 2010:1046)'s analysis of the Federal Trade Commission's (FTC) 2003 data, it appears that those at the greatest risk of ID theft victimisation are consumers between the ages 25 and 54, with higher levels of income (i.e., those with incomes greater than $75,000 which equals to R1 125 000 by the time of conducting this study), who reside in households headed by women with three or more children (Copes, Kerley, Huff and Kane, 2010: 1046). Holt and Turner (2012:311) add that most traditional university students fall within this age range, suggesting that there may be a high prevalence of ID theft among student populations. However, conversely, they mention that those with the lowest risk include the elderly i.e., those aged 75 and older.

McLoughlin (2015) argues that ID thieves target people who are struggling financially, telling them that they have won a prize or lottery, knowing that they will get so excited that they will participate in whatever scheme the fraudster has thought up. On the other hand, ID thieves will usually target people with a clean credit record, as it is easier to gain access to loans and open accounts using the personal details of someone who has already established a good payment track record. Miri-Lavassani *et al.* (2009:364-365) and Allison (2003) explain that the theft of IDs to commit forgery is not a new phenomenon in human societies. Contrary to this statement, Eisenstein (2008:1162) together with Hoar (2001: 295) contends that ID theft is a new phenomenon and a crime of the new millennium. As a result, Eisenstein (2008:1162) further asserts that the literature is not mature, and has indicated that additional research is needed.

The Causes of Identity Document Theft

The Canadian internet Policy and Public Interest Clinic [CIPPIC] (2007:10) expresses that one of the reasons for the causation of ID theft is that it offers thieves the possibility of a very high return combined with a very low risk of getting caught. Few individuals are ever charged with and convicted of identity theft-related crimes. A second key contributing factor to the growth of this crime is the ready access to personal information of individuals, from a variety of sources. Governments, hospitals, credit card companies, cell phone providers and other corporate entities regularly collect and store this information, sometimes without the knowledge and consent of the individuals concerned and not always with appropriate safeguards. Security breaches, especially from large data brokers, are a serious concern, and organisations may fail to notify affected individuals or cooperate with law enforcement agencies to limit the consequent damage.

Thukwana (2019) shares that the commercial crimes were on the rise, this prompted the South African organised business to call the private sector to become accountable for corruption and fraud [ID theft included], they were also requested to work with the local government and the South African Police Service (SAPS) to enhance the fight against the identity-related crimes. The 2018/2019 SAPS statistics showed a total of 83,823 commercial crimes, to record an increase of 14%. This included corruption, fraud, ID theft, forgery, embezzlement, and money laundering, as well as robberies and cash-in-transit heists [Not in order of importance]. For confirmation; Cele (2020) provides that commercial crimes, involving ID theft, fraud, scams, corruption, among others, increased by 0.1% in 2019/2020, as compared to 14.4% of 2018/2019 figures. Ironically to what often occurs in Hollywood movies; ID theft remains one of the greatest threats to South African consumers nor citizens. If the indicated past and recent statistics are anything to be considered, the ID theft [More especially theft of personal information] in this country becomes factual. The reported incidents increased by 200% over the last six years [2013-2019], costing the economy R1 billion loss annually (Law for All, 2020).

Bert-Jaap and Zeno (2009) present that with the continued recognition of the importance of identity and identity management in the information society, identity-related crimes are reported to be increasing. The combating of identity theft specifically is not only directed to the works of identity forensics; the policymakers are also facing challenges of policing this crime. Considerably; the importance of identity on the internet remains clear and digital identities give rise to identity-related crimes. A wide range of crime is committed using individual identities. The ID theft is touted as one instance involving multi-faceted categories of identity-related crimes. Other impediments relating to the conceptualisation of ID theft is witnessed, this lack of becomes evident when comparing the available data with various official and media reports on this subject. The limited common definitions of ID theft literature to aid in the related commissions of this crime compromise the operations of identity forensics to determine the real incidence of identity-related crimes.

Robinson, Graux, Parrilli, Klautzer, and Valeri (2011:11) state that with technology being the second leading cause of ID theft, it is clear that it has brought about new vulnerabilities. Such vulnerabilities are brought via unsecured personal computers and made existing identity infrastructures more vulnerable (e.g. by facilitating document forgery). Technology is a double-edged sword: it both changes and makes more efficient and effective how identity can be established, but also has similar effects on the way identity can be abused. Technology also permits new and sophisticated methods of committing existing crimes, such as through the use of the internet to perpetrate advance fee fraud or the distribution of fake phishing emails to dupe individuals into divulging personal data.

Newman and McNally (2005:46) have noted that ID theft has three main attractions for criminals: First, is the anticipated rewards; second, is the advantage of concealment which is intrinsic to the crime; and third, is the mild sentences compared with other crimes. Finch (2003: 94) emphasises that the internet provides unparalleled opportunities for those seeking a new identity to access the necessary information. One of the anomalies of internet use is that although *"it is much more difficult to verify identity and sincerity online...many users appear to be more trusting of those met online than those they encounter in person".* This leads internet users to be far less security-minded with their personal information when they are online than they are in 'real-life' situations.

According to White (2005:852), the rise of ID theft probably can be attributed to weaknesses in the structure in which personal information flows in society. The main weakness that identity thieves have exploited has been the "digital dossiers" of individuals. These dossiers contain personal information, including an individual's name, address, phone number, and Social Security Number (SSN) and are collected by various private and governmental organisations, such as banks, video stores, and the Department of Motor Vehicle Centres. A study by Buskovick (2013:7) has found that ID thieves may obtain victims' IDs through email phishing, stolen mails, data breach during a credit card transaction, internet scams, or a family member or friend who manipulates them into releasing their information. Buskovick found that about 3 in 10 agencies (29%) reported that victims very often have their IDs stolen through e-mail phishing and 49% of agencies reported that victim's IDs were obtained through internet scams.

The Measures to Mitigate Identity Document Theft

In responding to this crime; the forensic investigators confirm that this practice does not have a typical crime scene like other common crimes, where blood, fingerprints, and weapons can be easily seen nor identified. However, they are trained to trace forensic evidence, they know locations to inspect. The forensic investigators use the information at their disposal to inquire trails of money and data across international borders using complicated tunnels of technologies. Subsequently; the collaborative works of public and private sectors are currently versed in a vast range of fields, involving cybersecurity, forensic accounting, and digital evidence collection, among others. This unique specialisation can take a long time to complete, further requiring interactions of vast agencies and countries across the world, this calls for intelligence-led policing. It should be noted that this remains one of the difficult tasks for forensic investigators as large swathes of data are often stolen in a single operation to be transferred to a wide network of criminal accomplices for further dissemination of stolen data to other countries. The known nature of this crime involves the masking of one's identity, making it challenging to link potential perpetrators to this alleged crime. Many emphases are placed on preventing related attacks of this crime while attempting to recoup losses of outwitted victims (Forensics Colleges, 2020). According to Bert-Jaap and Zeno (2009), the key challenges of adequately responding to this crime rests on keeping up with technological developments, policymakers, and societal embracement of the changing world. With the ever-increasing importance of 'identity and identity management' and society's heavy reliance on information; the combating of identity-related crimes remains pivotal. It is revealed that the present [2020] information era [Fourth Industrial Revolution – 4IR] made it difficult to protect and secure an individual's personal information. This is brought by the ID theft struggle; this is regarded as a crime that causes great suffering to its victims. The offenders who are found guilty of this crime often use the ID of their victims for fraud purposes. Moreover, the social media also extended existing capabilities of people interactions and sharing of information, however, this is without appropriate guidelines to protect individuals from becoming victims of ID theft. Particularly, there are limited studies on the challenges of forensic technology in responding to ID theft and its contributory factors in South Africa in general and selected Polokwane area in particular. This crime is a crucial problem worldwide and an accelerating problem across South Africa (Michau, 2017).

The SAFPS and other identity forensics teams are working together to prevent fraud trends to dismantle them. This collaboration involves local and international large banks, retail groups, and insurance companies to reach their respective goals. This organisation also offers free protection to public members, especially the past victims of ID theft. This is done by uploading a victim's ID number and files to their database under this category 'Victims of Impersonation' to protect them against further attempts against them. In some cases, the details of the impersonator are uploaded on to this database. The consumers are also urged to pay close attention to the associated threats of fraudulent activity nor ID theft. Furthermore, the 'Personal Online Credit Report,' namely: 'My Credit Check' is launched to allow the users with valid ID numbers to monitor their complete financial history (Sihlangu, 2019). Technologically; biometrics and chip implants are cited to be going to provide a solution for the protection of personal identification. The chip implants can offer an economically and logistically viable option in this regard. Notable seminal studies are conducted on biometrics to offer improvements on authentications, however, the costs and logistics related to the implementations of biometrics present huge challenges. It is also noted that individuals should be physically present for this authentication process, in contrary, the biometrics do not provide an effective solution for electronic-commerce either. The human chip implants, which remains a very contentious issue, could also be considered as a possible solution of combating this crime either, as a person should also be present for identification and implants are therefore not a solution for personal online authentication, it is also confirmed that reputable reports from victims of this crime indicate that the commission of this crime was a life-changing event for them. Therefore, knowledge workers and internet users should practice privacy for their respective personal information. They should be aware of the associated risks and stay informed of available preventative measures. Thus, ID theft and privacy risk awareness training should form part of every organisation's training programmes and the available precautions should be linked with lifestyle change to safeguard personal information (Augustyn, 2005). The legislative framework such as the Protection of Personal Information Act (No. 4 of 2013) provides a legal right to confidentiality and individuals should be aware that unauthorised admission to information regarding a person's education, medical records, financial statements, criminal records, personal information or employment history is prohibited, South African Broadcasting Corporation [SABC] (2015) (in Michau, 2017). Thus, it is essential for individuals to know their rights regarding privacy and take their responsibility to guard their personal information. The workable solutions provided as good practices by Dirk (2015) (in Michau, 2017) include the following: "Never give a password or Personal Identification Number (PIN) telephonically, by electronic mail (e-mail) or via fax; do not transport redundant personal information in wallets or purses; avoid doing private banking by using internet cafes or insecure terminals; guard documents containing personal information and be sure to destroy them when these papers are not needed anymore and regularly check accounts and credit records to notice when strange transactions are made.”

Budhram (2012) highlights that there are many challenges to dealing with credit card fraud and [ID theft], since the related transactions do not require the physical presence of the rightful owner of the ID or stolen personal information, also regarded as a seller and purchaser notation. In response; the establishment of a dedicated joint working group consisting of members from the local SAPS Commercial Crimes branch, the National Prosecuting Authority Asset Forfeiture Unit (NPA AFU), and the local banks to address this crime holistically, it is believed that this may along vast innovative skills, expertise, and resources to effectively respond to this crime. The low conviction rates on ID theft indicate difficulties the local SAPS face in investigating identity-related crimes further calling for the implementation of an intelligence-led policing approach to respond to this crime.

According to Budhram (2012), the preventative countermeasures of credit card fraud [ID theft is no exception] suggests that "the vulnerability of the magnetic strip to skimming has resulted in banks replacing this technology with chip-and-pin technology;" this technology proved successful in countries such as the United Kingdom (UK), decreasing counterfeit card fraud by 32% in 2010-2011 respectively. In South Africa; not all cards have the-said chip-and-pin features as not all merchants have systems installed to support these cards, meaning the current magnetic stripe technology will continue to be used for the coming years. In following the international trends; the South African banks deployed sophisticated IT programmes that help to detect, prevent and reduce bank card fraud and ID theft, this includes the "Short Message Service (SMS) confirmation of transactions, the implementation of authorisation parameters, and thresholds, and forensic investigations." These measures are cited to reactive, rather than been proactive. To this course; the local banks should consider an intelligence-led policing approach to combating this crime. However, this approach can only be successful if the destroyed co-operation between the local SAPS and banks can be improved. This approach requires the combined use of crime analysis and criminal intelligence to determine crime reduction tactics to be offered against ID theft in this regard. Notably; the launch of 'online verification system,' which was a joint initiative between the Department of Home Affairs (DHA) and South African Banking Risk Information Centre (SABRIC), on 8 November 2011, this allowed the local banks access to the DHA National Identification System to verify the IDs of prospective and current clients, using their fingerprints. This tool provides an added benefit to the bank client in that it offers the banks a second layer of confirmation that the persons presenting IDs are indeed whom they claim to be.

In 2013, the South African DHS was in the process of implementing the Home Affairs National Identification System (HANIS). This system aims to replace the current paper system with a digital database. HANIS holds the ID numbers, fingerprints, and photos of South African citizens. HANIS can only work if those feeding information into it do so with integrity. If the levels of corruption are high within the DHA, then false information can easily be fed into the system (Smith, 2013). Furthermore, Newman and McNally (2005:68) divide the possible techniques for preventing ID theft into five categories as follows:

- Increase the effort the offender must make to complete the crime.
- Increase the risks of getting caught.
- Reduce the rewards that result from the crime.
- Reduce provocations that may encourage or otherwise tempt offenders.
- Remove excuses that offenders may use to justify their crimes.

White (2005:854) submits that as instances of ID theft have increased, so have the measures taken to prevent theft. Generally, these measures can be classified into three groups. The first has been for individuals to take greater responsibility in protecting their personal information. The second measure is the creation of criminal statutes to punish identity thieves, and the fourth measure has been to allow civil remedies based on claims of invasion of privacy and breach of confidentiality.

In addition to the above, Albrecht, Albrecht, and Tzafrir (2011:407) state that some of the most effective proactive ways for a consumer to minimise their risk to ID theft include the following:

- Guard mail from theft. When away from home, have the postal service hold your mail.
- Guard SS cards and numbers. An individual’s SS number is valuable information for any ID theft perpetrator. With knowledge of someone's Social Security number, perpetrators can open all kinds of new accounts in the victim's name. Therefore, consumers should always keep their SS card in a safe place.
- Safeguard all personal information. Safeguarding personal information is very important for every individual. Consumers, who have roommates, employ outside help to clean or perform other domestic services or have outside people in their house for any reason need to be particularly careful.
- Guard trash from theft. Consumers need to tear or shred receipts, insurance information, credit applications, doctor’s bills, checks and bank statements, old credit cards, and any credit offers they receive in the mail, as well as any other source of personal information. Buying a shredder is one of the wisest purchases individuals can make.

- Protect the wallet and other valuables. Consumers should carry their wallets in their front pocket and never leave it in their car or any other place where it can be stolen. It is important for consumers to always be aware of where their wallet is and what its contents are. Individuals should only carry identification information and credit and debit cards that they regularly use in their wallets.
- Protecting the home. Consumers should protect their houses from perpetrators. Some perpetrators have been known to break into a home and not steal a single physical object. The victims may not even know someone has been inside their home. The perpetrator will steal all information that is needed to easily commit identity theft and then leave. To prevent this from happening, it is important to lock all doors, preferably with deadbolts or double locks, and lock all windows. It is a good idea to have an alarm system.

RESEARCH DESIGN AND METHODOLOGY

Welman and Kruger (2001:46) define a research design as a plan through which the researcher attains research participants or subjects to collect information from them. Offering a closely related definition to this is Babbie (2007) quoted by De Vos, Strydom, Fouché, and Delport (2011:142) states that "… a research design is a process of focusing your perspective for a particular study". Most significantly, according to Durrheim (2006:37), when developing a research design, the researchers should consider the purpose of the research, the theoretical paradigm informing the research, the context or situation within which the research is carried out and the research techniques employed to collect and analyse data, which should be taken into account when conducting a study. In connection to this statement, the researchers obtained, *inter alia*, statistics pertaining ID theft published by the SAFPS and SABRIC, the recent methods employed by various syndicates to unlawfully and intentionally commit misrepresentation using other persons' IDs for their financial gain, and the SAPS strategic plan in curbing ID theft. The availability of this evidence, although to a limited extent, assisted the researchers to address the research problem, and the following hypotheses guided this study: *Hypothesis 1*: The awareness level of SAPS and other relevant stakeholders on the crime of ID theft is responsible for its increasing rate in the Polokwane policing area. *Hypothesis 2*: ID theft would be effectively curbed in the long-run if the root causes of the problem are addressed. *Hypothesis 3*: The SAPS has not been effective in the prevention of ID theft in the Polokwane policing area.

This study was conducted in Polokwane, the capital city of Limpopo Province. To cover the selected location as well as the target population, specific areas were identified within and surrounding the city, namely, Polokwane CBD, and the following residential areas surrounding Polokwane: Flora Park and Bendor Park. Due to the complexity of the study location, it was essential to sample the target population from the inner city including the surrounding residences. Further methodology pursued to complete this study included *inter alia*, the following: study population, sample size, and procedures. Research can be classified in terms of their purpose. Accordingly, they are most often classified as exploratory, descriptive, explanatory, correlation, evaluation, intervention, and action research (De Vos *et al.* 2011:95-99).

This study employed descriptive research to give a comprehensive understanding of the crime of ID theft in Polokwane. Furthermore, an explanation of how the data collected was analysed, limitations relating to the problems encountered during the data collection process were pointed out, the reliability and validity process, and ethical considerations were highlighted in this section. Furthermore, from the different available research approaches, namely: qualitative, quantitative, and mixed-method approach, the researchers used the quantitative approach. Quantitative research makes use of questionnaires, surveys, and experiments to gather data that is revised and tabulated in numbers, which allows the data to be characterised by the use of statistical analysis (Schulenberg, 2007:1). The latter author goes on to say that quantitative researchers measure variables on a sample of subjects and express the relationship between variables using effect statistics such as correlations, relative frequencies, or differences between means; their focus is to a large extent on the testing of theory.

Through this study; in-depth knowledge of how the SAPS responds to ID theft was acquired. Rather than focusing on ID theft in its broad scope, the researchers narrowed the study with a specific focus on Polokwane CBD, Bendor Park, and Flora Park, including the number of stores situated in the business sectors of these areas.

Methods of Data Collection

The researchers utilised two scientific methods to collect data. Primary data was collected through the use of survey method (questionnaires) and secondary data through consultation of literature. Irrespective of the high traveling costs and the large geographical area, questionnaires were delivered by hand to the respondents. In the case of those respondents who requested extended time to complete the questionnaire, a maximum of 48 hours (two days) to complete the questionnaires was afforded to them. The researchers chose to follow this practice to give the respondents sufficient time to analyse and understand the questionnaire.

Questionnaire (Primary Source)

In collecting data from the targeted groups, questionnaires were distributed to a sample of police officials in Polokwane and members of the public residing within the jurisdictional areas in which the station operates. These areas were limited to Polokwane CBD, Bendor Park, and Flora Park (This included the number of stores situated in the business sectors of these areas).

Section A, which is the first part of the questionnaire, consists of biographic details of the respondents, which as well covered members of the SAPS. It was inclusive of the following: (1) Age group, (2) gender, (3) marital status, and (4) if SAPS official, (5) experience, and (6) rank. As a point of departure, it was important for the researchers to determine and ascertain if the public is even aware of the crime of ID theft, thus section B was subsequently developed (7) – (13). The researchers found it necessary for the populace to understand the likely causes of ID theft and developed section C (14) – (20). Community policing has become a new concept within the policing spectrum, and it was believed by the researchers that it is necessary to evaluate and assess the level of police partnership with the community and this was addressed in section D (21) – (24).

As revealed in Table **1**, it was understood by the researchers, the nature of ID theft posed challenges in responding positively and timeously to this crime, and it was, for this reason, that section E (25) – (28) and section F (29) – (31), were developed respectively. Communication channels will always play a vital role in reporting and conveying information regarding any crime. In this regard, section G (32) – (36) was constructed. Furthermore, it is general knowledge that for a specific crime to be committed various methods must have been used and so the law also must have been broken. Section H (37) – (40) was constructed to address that. The researchers concluded the questionnaire with a general statement (41) for general comments. It is also significant to indicate that not all of the questionnaires that were distributed and returned formed part of the study. Only 69% (90) of the distributed questionnaire was correctly completed and utilised for this study.

A total of 29% (26 respondents) made comments. Some of the respondents made comments about more than one issue[1]. The questionnaires were distributed to the identified target groups as identified by the researchers and were both self- and group administered.

From Figure **1**, it can be deduced that of 90 the questionnaires utilised for this study; 23 respondents made comments and 64 did not comment. As already stated, whether completed or not, this section was not taken into consideration when determining and validating the correct completion of the questionnaire, as this section was explained to the respondents to be optional.

Literature (Secondary Source)

Because the credibility of sources is of most importance in this regard, this study searched for literature worthy of review and that assisted the researchers in achieving the research objectives and answering the hypotheses. The researchers made use of extensive literature from within South Africa and around the globe to determine the extent of research conducted on ID theft and also, what the contributing factors are, relating to the growth and causes of ID theft.

The researchers relied heavily on sources in the legal, policing, and investigation of crime fraternities, as primary sources of literature. To validate the data received, literature was also gathered from other secondary sources including relevant journal articles, published dissertations, and theses, legislations, statistics, monographs published by the Institute for Security Studies (ISS), articles from accredited scientific journals, and media articles relevant to the

[1] Take note that the last section on general comments (statement 41), whether completed or not, was not taken into consideration when determining and validating the correct completion of the questionnaire, as this section was explained to the respondents to be optional.

Table 1: Response Rate

Target Population	Sample Size		No. of distributed questionnaires	No. of returned questionnaires		No. of correctly completed questionnaires	
	No.	%		No.	%	No.	%
Polokwane Police Station:							
Detectives	15	11.55%	15	15	12.7%	15	17%
SCP	10	7.70%	10	10	8.5%	10	11%
Records	03	2.30%	03	03	2.5%	03	3%
Community Service	02	2.55%	02	02	1.7%	02	2%
Total	30	23.05%	30	30	25%	30	33%
Polokwane Residents:							
Flora Park	35	26.90%	35	30	26%	20	22%
Bendor	35	26.90%	35	29	24.5%	27	30%
Polokwane CBD	30	23.10%	30	29	24.5%	13	15%
Total	100	76.95%	100	88	75%	60	67%
Grand Total (%)	130	100%	130	118	100%	90	100%

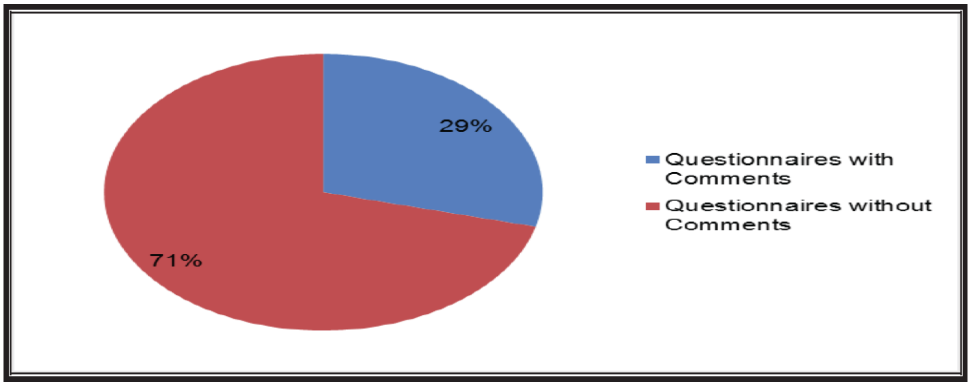

Figure 1: Percentage of comments made by respondents (N=90).

matter under investigation. Throughout the research, attention was more directed on similarities and anomalies which addressed the research objectives and hypotheses. The hypotheses were used to focus the search for relevant seminal information on this subject.

Study Population

It could have been ideal to conduct this study with all the police officials in Polokwane attached to the Provincial Commercial Crime Unit (CCU) based in the city to obtain the true answer to the research problem because these officials are engaged and deal with ID theft on a higher level (as they deal with cases amounting to more than R30 000 in monetary value). Practically, it was not possible to interview all of the police officials owing to a prolonged approval process from the Directorate for Priority Crime Investigation (DPCI) to grant such officials permission to part-take in the study.

To represent the population, the researchers decided to take as target population the officials of Polokwane Police Station varying from respective components, managers of various stores within the inner city, including members of the DHA, as well as members of the public residing at the selected residential locations of the study.

This was because the researchers were familiar with the study locations and reside around the proximity of identified areas. It was therefore easier for the researchers to access officials at the Polokwane and members of the public residing in these areas.

Sample Size and Procedure

A total of 30 police officials at Polokwane were sampled, exclusive of administrative staff. The sample included 15 local SAPS Detectives, 10 members of the SAPS Social Crime Prevention (SCP), 03 from records, and a further two from community services. The sample drawn from the target population was achieved by randomly selecting officials with various ranks within the division.

Through the snowball sampling method, the researchers identified four categories or sections at the Polokwane, namely: detectives, members of SCP, police officers at the records section, and from community services, with various ranks attached to them (Warrant and Constables, just to name the two, with vast experience on ID theft case). The focus on these non-commissioned officers was driven by their daily involvement in cases of ID theft and their experiences in dealing with such cases. Even though these are operational level positions, only officials with 10 or more years of experience were targeted.

Figure **2** shows the target population, as well as sample distribution. The following demographic variables have been used in this study:

- Age (applied to members of the public only).
- Gender.
- Years of service and (applied to the SAPS members only).
- Rank (applied to the SAPS members only).

Figure **2** presents that among SAPS members, 30 respondents were a target and participated as expected by the researchers, and 60 public respondents were utilised in this study.

According to the sampling guidelines provided for by De Vos, *et al.* (2011:225), 45 respondents from a targeted population of 100, is sufficient to draw reliable results. In this research, the initial targeted population was 130, the result of which turned out to be that 90 respondents correctly filled the questionnaires and the other 40 were disqualified due to errors and non-completion. In this light, these 90 respondents were sufficient to draw reliable results as stated by De Vos, *et al.* (2011:60).

Figure **3** indicates that 50 percent of the total respondents are detectives, 33 percent perform SCP functions, 10 percent are records personnel, and 7 percent are members working in the Community Service Centre (CSC). Members working in the CSC are those members referred to as the face of the station. They are the first to know that a crime has

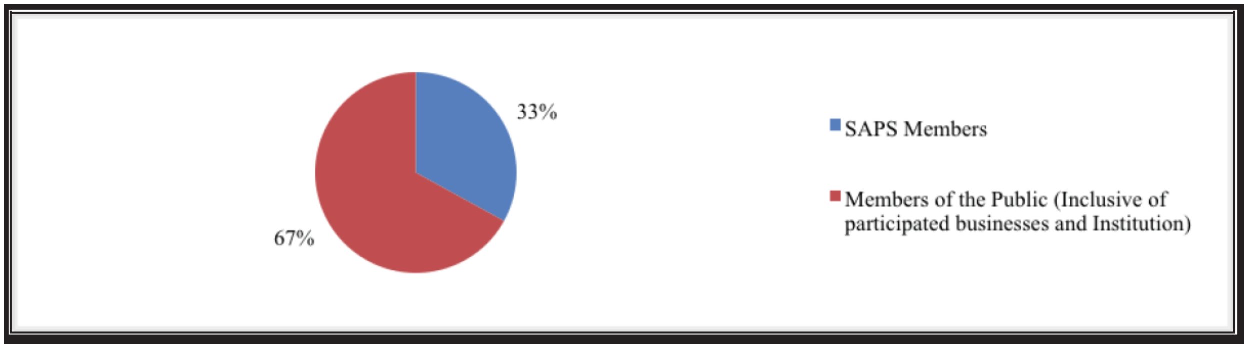

Figure 2: Target Population (N= 60 Public Respondents; N=30 SAPS; N=90).

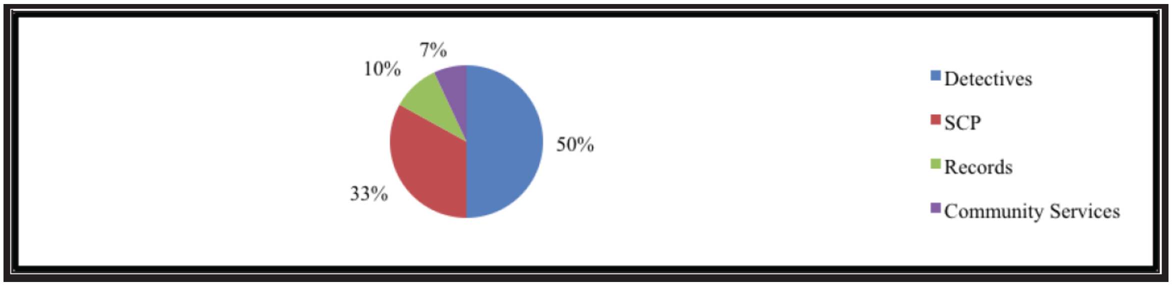

Figure 3: Component division.

been committed and are responsible for the initial completion of the relevant documentation and docket, which will be used at a later stage by the detective assigned to the case. After completion of these documents, the CSC members keep the docket safe for the assigned detective. Other documents are also kept in this office for record-keeping. Once a crime has been committed and a case opened, a detective is assigned to the case. The detective undertakes the investigation process. The assigned detective identifies the possible leads, gathers evidence and interviews, and interrogates witnesses where necessary. If a suspect is identified, the detective will then apprehend the person and bring the person before the court as prescribed by the Criminal Procedure Act [CPA] (No. 51 of 1997). The Polokwane SAPS Police Station has a division, which is responsible for social crime prevention. It is the responsibility of this division to perform crime prevention patrols at specific locations within the station jurisdiction, which includes the three identified areas in this study. The division conducts visible policing in these locations.

Method of Data Analysis

The data obtained from the study were analysed using Microsoft Excel and the Statistical Package for the Social Sciences (SPSS) to derive counts, averages, and percentages. The data results are presented in tables and graphs. Some of the results are presented using the explanatory text. The researchers read data several times to get a perspective and discussed data in an interpretative manner. The numeric and graphical data were constructively interpreted to give the prospective reader a clearer sense of the results.

STUDY RESULTS: DATA PRESENTATION, ANALYSIS, AND INTERPRETATION

The research hypothesis explored in this section concerns the root cause of ID theft. Data regarding the probable causes of ID theft are presented in Tables **2** and **3**, as well as Figures **4**, **5**, and **6**. The results presented in this section also cover Section C of the questionnaire.

Data presented in Table **2**, indicate that the majority of the respondents (68%) regard the lack of understanding of ID theft as an important causative factor of ID theft. The responses of both the SAPS and public members were weighed against each, and the majority shared the same consensus on this subject. This indicates that both police officials and the public find difficulties in comprehending ID theft. An effective response to this crime may be achieved if police officials understand the type of crime they are dealing with and if the public understands what type of crime they need to prevent themselves against. Expert education to the public and police then plays a significant role in this regard. Practically, crime statistics have shown that ID theft is not a common crime. This suggests that ID theft is a sophisticated type of crime, committed by literate and high profiled individuals, mostly aimed at financial gains. To best understand ID theft, police need to be trained by experts in the field of commercial crimes continuously.

To be able to prevent and respond to ID theft, potential victims and SAPS officials must understand what they are dealing with. By merely understanding the concept will enhance ways of preventing and responding to ID theft. It appeared from the results that more than two-thirds (68%) understand the concept of ID theft; however, some disagreed (21%) that people's

Table 2: Lack of Understanding of the Concept “Identity Document Theft” (N=90)

Respondents	Agree	Strongly Agree	I do not know	Disagree	Strongly Disagree	Grand Total
Public	14 (16%)	26 (29%)	7 (8%)	5 (6%)	8 (9%)	60 (67%)
South African Police Service (SAPS)	5 (6%)	15 (17%)	4 (4%)	4 (4%)	2 (2%)	30 (33%)
Grant Total	19 (22%)	41 (46%)	11 (12%)	9 (10%)	10 (11%)	90 (100%)

Table 3: How Stolen Identity Document Theft are Obtained: A Case Study of Polokwane, South Africa (N=90)

Statement	Agree	Strongly Agree	I do not know	Disagree	Strongly Disagree	Grand Total
The loss of wallets	31 (34%)	45 (50%)	7 (8%)	2 (2%)	5 (6%)	90 (100%)

lack of understanding of ID theft does not contribute to its cause. A total of 12% of the population did not know.

Data as presented in Table **3**, reflect the views of the respondents regarding the loss of wallets as one of the influential factors underlying the cause of ID theft in the Polokwane policing area. Respondents were asked to report on how ID theft victims had their information stolen and they were tested on one method, namely: the loss of wallets. Slightly more than one third (34%) of the respondents agreed with the statement that the loss of wallets is one of the methods through which their IDs are obtained and further supported by half of the population (50%) who strongly agreed with this view. Only 2% disagreed and 6% strongly disagreed. A total of 7 in 90 (8%) respondents did not know how their IDs are obtained.

From these results, it can be seen that the majority of the respondents (84%) believe that the loss of wallets gives rise to ID theft. This finding suggests that most victims know how their IDs are or were stolen. The study by Buskovick (2013:7) indicated that most of the respondents, over one-third (49%) cited stolen wallets or purse, as the most frequent method of losing their IDs. Based on the total 7% of respondents who disagreed, it can be suggested from this finding that there are other ways in which IDs may be stolen. Buskovick (2013:7) study has alerted that ID thieves may obtain victims' IDs through email phishing, stolen mails, data breach during a credit card transaction, internet scams, or a family member or friend who manipulates them into releasing their information. The latter method implies that perpetrators may often be the people known and close to the victims. It was also found that, between both genders, only a minority (7%) of the population did not know how their IDs might be stolen.

The graphical data above present perceptions of public and SAPS respondents regarding the role of technology as a cause of ID theft. Interestingly, 36.7% agreed and almost half of the respondents strongly agreed that technology is amongst the root causes of ID theft. Generally, close to three-thirds majority 82.3% of the respondents share similar views that technological developments give rise to ID theft. This finding indicates that advancing technology makes the work of ID thieves much easier to achieve their criminal goals.

In today's world, people must keep up with technology to conduct their daily routines. They are required to adapt daily to new knowledge and exciting discoveries that are constantly changing the way they live and do business. Technological advances now allow people to carry out the most ordinary tasks, such as ordering groceries from the store to the most complex activities, such as performing complicated surgery, all from a separate, remote location: a computer connected to the internet. All these activities will require the consumer to punch in their ID numbers for the transaction to go through. Conversely, only a few (10%) of the respondents did not regard technological advancement as a causative factor of ID theft. Almost 7 in 90 respondents (7.8%) did not know how technology contributes to the theft of IDs.

The data on Figure **5** presents the results of perspectives of respondents by age regarding whether access to the internet is fundamental to the commission of ID theft. Although the internet may be seen and understood to be part of technology, the researchers found it significant to present the results on this concept solely because access to the internet is predominantly a departing point in cases where ID theft is committed with other technological equipment.

As can be seen from the results, between the ages of 18 and 25, 1% agreed, 3% strongly agreed and 1% did not know. Between the ages of 26 and 35, 9% agreed, 17% strongly agreed, 8% disagreed, 2% strongly disagreed and only 4% did not know. From the ages of 36-45, 10% agreed, 20% strongly agreed, 6% disagreed, and similarly the other 6% strongly disagreed. Only 1% did not know. Moreover, 3% of

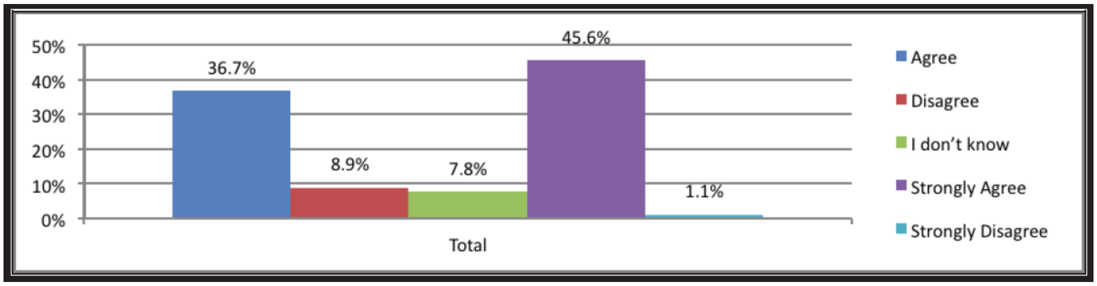

Figure 4: Technological advancement (N=90).

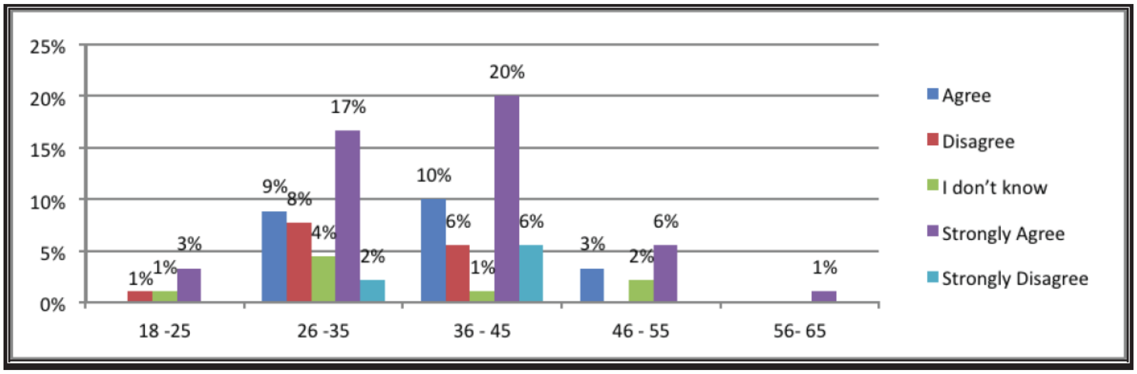

Figure 5: Respondents' views by age: access to the internet (N=90).

ages from 46-55 agree, 6% strongly agreed, whilst 2% carried no knowledge. To conclude, only 1% of the ages of 56-65 strongly agreed.

From the survey, it was found that respondents between the ages of 18 and 45 frequently access the internet and are likely to become victims of ID theft. A total of two-thirds majority (60%) concurred that access to the internet promotes ID theft. Supporting this finding are the findings in Buskovick (2013:7) study, where about 3 in 10 agencies (29%) reported that victims very often have their IDs stolen through e-mail phishing and 49% of agencies reported that victims' IDs were obtained through the internet frauds. Further to this, it is clear that in this modern world, life without the internet would be a serious challenge as the majority of the people are internet reliant. On the other hand, exposure to the risks of falling victims of ID theft has increased.

It cannot be disputed that the internet has grown into a vast electronic network that now runs the entire globe, and it will only continue to grow. Because people use the internet in their everyday lives, they rely on it for a safe and accurate exchange of information. Constantly, personal data such as ID numbers, credit card numbers, and passwords are traveling through wires, and through the air, from one computer to another. With security measures in place to protect this sort of information online, most people feel safe on the internet and trust that their personal information will remain confidential. But, unfortunately, criminals have also adapted to advancements in technology and, these days, people are becoming victims of crimes committed over the internet.

Figure **6** shows the views of the respondents regarding ignorance on the part of individuals contributing to the growth of ID theft. Almost the majority of the respondents carried similar views. When asked to respond to this view, 36% agreed and 52% strongly agreed, while 7% disagreed and only 3% strongly disagreed. The results further indicated that of the total population, 2% did not know.

In summary, the results showed how people are ignorant in handling their IDs, and thus greatly more than a two-thirds majority (88%) of the population supported this perspective. This finding was a bit surprising given the finding in Figure 4.4, where the results indicated that nearly two-thirds majority (57.8%) knew the consequences of ID theft. Based on this finding, it is therefore surprising to find that despite people knowing what the consequences of ID theft are, they remain ignorant in safekeeping their IDs. On the contrary, 9 in 90 respondents (10%) did not agree that

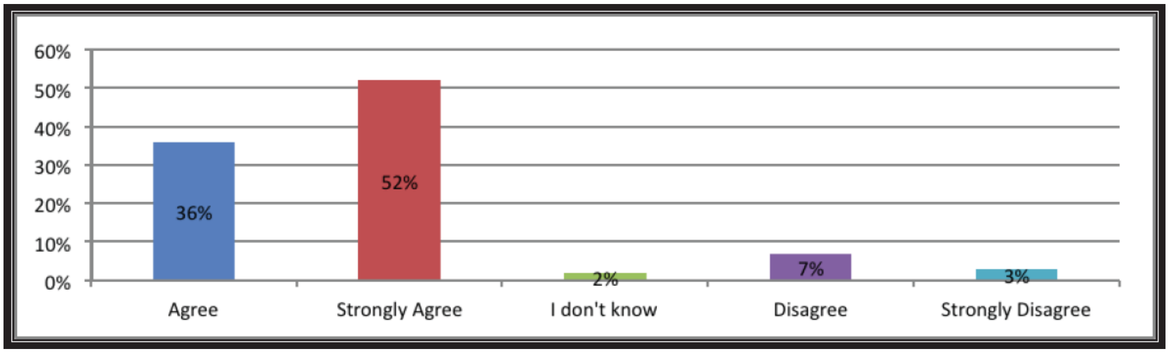

Figure 6: Individuals' ignorance and Identity Document theft (N=90).

people's ignorance is amongst how they lose their IDs and consequently leading to ID theft. Allison, *et al.* (2005:19) state that the prevalence and impact of identity-based crimes have grown significantly in the last decade and relatively little is known about the nature and extent of these activities. Holt and Turner (2012:309) suggest that perhaps, more importantly, even less is known about how individuals identified as high risk for ID theft victimisation can protect themselves from experiencing such an incident. The findings in this study lend partial support to these researchers' views. Although some were not aware of ID theft, the findings have shown that the majority are aware of the existence of this crime however, they are unknowledgeable.

Consulted statistics, ID theft research institutions, and law enforcement officers proposed that ID theft is on the rise. To support this perception, the finding in this study has shown that the majority of SAPS officials and Polokwane residents have accepted that ID theft victims are many. Although prevalence rates of ID theft are on the rise, they remain a relatively rare event (Holt and Turner, 2012:308).

Irrespective of the findings of this study indicating that the majority of people are aware of ID theft, particularly those between the ages of 26 to 45, the researchers reviewed empirical studies and identified that victims of ID theft are many across the globe. Supporting these findings, McLoughling (2015:2) reports that in South Africa there were 15420 victims of impersonation records listed in the SAFPS database as of 31 December 2014, with 3334 cases reported in 2014 alone. On the other hand, in the United States (US), it was also revealed that ID-related theft was “at a record high” and happened every 3.5 s on average and Federal Trade Commission **(**FTC) reported 8 million ID theft victims in 2006 and a similar finding of 8.1 million victims was found in 2007. The number of identity theft victims climbed to 9.9 million in 2008 (Lai, Li, and Hsieh, 2012). Although a comparison between males and females regarding the most vulnerable gender concerning ID theft was not shown in the findings, literature shows that males appeared to be less resilient to ID theft victimisation in keeping with previous research on the gender dynamics of ID-based crimes and fraud (Copes *et al.,* 2010:2).

In line with the presentation made on the literature review section, it can be deduced that the causes of ID theft are many and much attention should be invested to curb this scourge effectively; this study found the following in this regard:

- There is a need to provide the SAPS members with ID theft training and Polokwane residents with education on ID theft and other related financial crimes that may occur as a result of ID theft.
- Victims are careless in handling their personal information since the loss of wallets was found to be a frequent manner by which victims lose their IDs, however, very often the victim does not know how the perpetrator obtained his or her ID.
- Access to the internet and technology are the most factors simplifying the stealing of personal information.
- Individuals aged 26 to 45 are vulnerable to ID theft as they are found to be accessing the internet more frequently than other ages and are likely to be subjected to financial exploitation.
- From the latter conclusion, it can also be deduced that such victims do not report this crime to SAPS as they may not be aware of their victimisation.
- And again, by the use of the internet, it becomes difficult to identify the perpetrator and for SAPS to investigate the crime due to its complex nature.
- Finally, it can be concluded that people are ignorant about keeping their IDs safe and destroying their personal information.

CONCLUSION AND RECOMMENDATIONS

The findings of this study as tested against the hypotheses, many of which confirm the need for police to keep up to date with technology, many of which indicating the need for continued and enhanced awareness should be staged to understand the causes of ID theft in Polokwane policing Area; the highlighted recommendations below marks the conclusion to this study as well:

- In as far as knowledge about ID theft is concerned, the respondents are aware of ID theft. There are those few, constituting minority, who do not about this crime.

- The majority of the respondents from both the public and the SAPS members report ID theft. This consequence concludes that there is a high number of victims of ID theft.

- A further conclusion to the above could be that, males are less targeted by perpetrators of ID theft and the existing possibility is that males do not report this crime.

- It can further be concluded that, due to the nature of this crime, victims do not know if fraud is committed in their names and only when the damage has already been done, they become aware.

- Concerning age, those aged 26 to 45 years are at high risk of becoming victims of impersonation and those at the age of 18 to 25 and 56 and above are likely at low risk.

- The majority of the respondents know the consequences of ID theft while on the other hand it cannot be ignored that there are people who do not know the impact of ID theft.

- Regarding campaign awareness, only specific and not all areas are targeted by SAPS to conduct ID theft awareness.

- Additionally, although there is a high level of awareness, there is still a need to increase police and public knowledge about ID theft.

After having measured the results obtained from the data and the conclusions made upon analyses of the findings in this study, it is now important to discuss these findings and conclusions by incorporating what research had already been conducted to the results in this study, as this might be helpful to begin to identify several areas of concern relating to ID theft, not in Polokwane, but within the province of Limpopo as well.

This study has generally found that cases of ID theft are reported to the police and that people are aware of this crime. While on the other hand, other people did not know about the existence of this type of crime and what to do in case they find their IDs unlawfully utilised to commit other crimes. Although many carried the knowledge of this crime, it was apparent that most did not know how to prevent themselves from being victimised. With that said, the question is whether the SAPS in Polokwane can respond to this crime? Therefore, the purpose of this study was to examine the SAPS's ability to respond to ID theft in Polokwane.

The findings of this study should be used to disseminate awareness on ID theft, including educational and victim assistance programmes. The SAPS should undertake educational programmes and use the findings of this research to assist in describing what impacts ID theft has on victims and how the latter may prevent themselves against ID theft. Educational programmes in this area (Polokwane) would typically include a discussion between the SAPS members and the community regarding the financial effects of ID theft on victims.

Based on the findings of this study, educational programmes should include an overview of information on the possibility of the existing possible opportunities of being a consistent victim of ID theft. The SAPS in Polokwane Police Station should explore ways to educate and remind Polokwane residents about ID theft prevention. They can use Polokwane local newspapers, local radio stations, and the SAPS web page to publicise information. Pamphlets should be developed and distributed to local businesses, churches, taxi ranks, banks, shopping malls, Facebook, and other social media. The SCP members and Community Policing Forums (CPFs) should be encouraged in finding opportunities to inform residents on prevention techniques.

REFERENCES

Albrecht, C., Albrecht, C and Tzafrir, S. 2011. How to protect and minimise consumer risk to identity theft. *Journal of Financial Crime,* 18(4). https://doi.org/10.1108/13590791111173722

Allison, SFH. 2003. A case study of identity theft. Published MA Dissertation, University of South Florida, United State. Available at: http://scholarcommons.usf.edu/etd/1322. [Accessed: 2014.08.05].

Allison, SFH., Schuck AM and Lersch, KM. 2005. Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice,* 33: 19-29. https://doi.org/10.1016/j.jcrimjus.2004.10.007

Angelopoulou, O. 2010. Analysis of Digital Evidence in Identity Theft Investigations. Published PhD Thesis, University of Glamorgan, United Kingdom.

Augustyn, D. 2005. Identity theft escalation - You may need to change your life. *South African Journal of Information Management*, 7(4), 1-11. https://doi.org/10.4102/sajim.v7i4.284

Bert-Jaap, K and Zeno, G. 2009. Identity-related crime and forensics. Berlin, Germany: Springer.

Budhram. T. 2012. Lost, stolen or skimmed - Overcoming credit card fraud in South Africa. *South African Crime Quarterly* No. 40, 31-37.

Buskovick, D. 2013. Financial Crime and Identity Theft: Law Enforcement Response, Challenges and Resource Needs. Report of Minnesota Law Enforcement Identity Theft Survey. US: Minnesota Department of Public Safety.

Canadian Internet Policy and Public Interest Clinic. 2007. Techniques of Identity Theft. CIPPIC Working Paper No.2 (ID Theft Series). Ottawa: Canadian Internet Policy and Public Interest Clinic.

Cassim, F. 2015. Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? *Potchefstroom Electronic Law Journal/ Potchefstroomse Elektroniese Regsblad (PER / PELJ)*, 18(2), 69- 110. https://doi.org/10.4314/pelj.v18i2.02

Cele, B. 2020. Minister Bheki Cele: Annual Crime Statistics 2019/2020. 31 July, South African Government [Omline]. Available at: https://www.gov.za/speeches/minister-bheki-cele-annual-crime-statistics-20192020-31-jul-2020-0000.

Copes, H., Kerley, K.R., Huff, R and Kane, J. 2010. Differentiating identity theft: An exploratory study of victims using a national victimisation survey. *Journal of Criminal Justice* 38: 1045–1052. https://doi.org/10.1016/j.jcrimjus.2010.07.007

De Vos, A.S., Strydom, H., Fouché, C.B and Delport, C.S.L. 2011. *Research at Grass Roots: For the Social Sciences and Human Service Professions*. Pretoria: Van Schaik.

Department of Justice, South Africa. 1977. *Criminal Procedure Act (Act No. 51 of 1977).* Available at: http://justice.gov.za/legislation/acts/1997-105.pdf [Accessed on: 2015.06.05].

Durrheim, K. 2006. *Research design*. In Terre-Blanche, M., Durrheim, K and Painter, D. *Research in practice: applied methods for the social sciences.* Cape Town: University of Cape Town.

Eisenstein, E.M. 2008. Identity theft: An exploratory study with implications for marketers. *Journal of Business Research,* 61. https://doi.org/10.1016/j.jbusres.2007.11.012

Finch, E. 2003. What a tangled we weave: Identity theft and the Internet. England: Willan.

Forensics Colleges [Online]. 2020. Follow the money: Identity theft. Available at: https://www.forensicscolleges.com/blog/follow-the-money/identity-theft.

Hinde, S. 2005. Cyber-terrorism in context. *Computer Fraud and Security*. 22(1). https://doi.org/10.1016/S1361-3723(05)00148-X

Holt, TJ and Turner, MG. Examining Risks and Protective. 2012. Factors of On-Line Identity Theft. *An Interdisciplinary Journal,* 33(4). https://doi.org/10.1080/01639625.2011.584050

Joseph, N. 2013. Identity Document theft ‘costing SA millions’. IOL news [Online], 2 June. Available at: http://www.iol.co.za/news/south-africa/iedentity-theft-costing-sa-millions-1.403125.

Koops, B., Leenes, R., Meints, M., Van der Meulen, N and Jaquet-Chiffelle, D. 2009. A Typology of identity related crime. *Information, Communication and Society,* 12(1): 1-24. https://doi.org/10.1080/13691180802158516

Lai, F., Li, D and Hsieh, C. 2012. Fighting identity theft: The coping perspective. *Decision Support Systems,* 52(3). https://doi.org/10.1016/j.dss.2011.09.002

Law for All [Online]. 2020. Identity theft in SA: Fact or fiction? Available at: https://www.lawforall.co.za/uncategorized/identity-theft-south-africa-law/.

McLoughlin, C. (carolm@safps.org.za). 2015. ID theft Statistics. [E-mail to:] Rakololo W.M. (moyahabo.rakololo@gmail.com) August 5.

Michau, N. 2017. Identity theft risk quantification for social media users. Master of Engineering (Industrial Engineering) in the Faculty of Engineering. Stellenbosch: Stellenbosch University.

Miri-Lavassani, K., Kumar, V., Movahedi, B and Kumar, U. 2009. Developing an identity fraud measurement model: a factor analysis approach. *Journal of Financial Crime*, 16(4). https://doi.org/10.1108/13590790910993708

Murphy, KP. 2003. Identity theft: assisting victims in their recovery. E.M.U. School of Police Staff and Command: Flat Rock Police Department.

Newman, GR and Mcnally, MM. 2005. Identity Theft Literature Review. United States: Department of Justice.

Roberds, W and Schreft, SL. 2009. Data breaches and identity theft. *Journal of Monetary Economics*, 59(1). https://doi.org/10.2139/ssrn.1296131

Robinson, N., Graux, H., Parrilli, DM., Klautzer, L and Valeri, L. 2011. Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report. United Kingdom: Rand Europe.

Ruppar, CA. 2005. Identity theft prevention in cyberciege. Published MSc. Dissertation, Naval Postgraduate School Monterey: California.

Schulenberg, JL. 2004. Policing young offenders: A multi-method analysis of variations in police discretion. Canada: University of Waterloo.

Sihlangu, J. 2019. Identity fraud and theft on the rise in South Africa compared to 2018. Pretoria: The South African.

Smith, T. 2013. Identity theft. Available at: http://www.bowman.co.za/eZines/Custom/Litigation/MarchNewsletter/IdentityTheft.html.

South African Fraud Prevention Service. 2020. 02 identity theft. Available at: https://www.safps.org.za/Home/FraudPrevention_CommonFraudScams.

Staff Writer [Online]. 2019. Big increase in identity fraud cases in South Africa. 19 September, BusinessTech. Available at: https://businesstech.co.za/news/technology/342057/big-increase-in-identity-fraud-cases-in-south-africa/

Thukwana, N. 2019. 19 September, Sunday Times [Online]. Crime Stats: Sharp rise seen in commercial crimes. Available at: https://blsa.org.za/crime-stats-sharp-rise-seen-in-commercial-crimes-bac/.

White, AE. 2005. The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It? *Marquette Law Review* 4(8): 847-866.

Received on 06-08-2020 Accepted on 21-09-2020 Published on 01-10-2020

DOI: https://doi.org/10.6000/1929-4409.2020.09.64